UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/929,178 | 08/14/2001 | Donald P. Matthews JR. | 2875.0500001 | 8980 |

26111 7590 10/13/2010

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

| EXAMINER | |
|---|---|
| POPHAM, JEFFREY D | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2491 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 10/13/2010 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/929,178 | MATTHEWS, DONALD P. | |
| | Examiner | Art Unit | |
| | JEFFREY D. POPHAM | 2491 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *02 August 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *2,3,28-30,32-36,45 and 46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2,3,28-30,32-36,45 and 46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 June 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## *Remarks*

Claims 2-3, 28-30, 32-36, and 45-46 are pending.

## *Response to Arguments*

1. Applicant's arguments filed 8/2/2010 have been fully considered but they are not persuasive.

Applicant argues that Howard does not teach “performing authentication operations on a set of header data and the payload data … performing encryption operations on a set of data in the payload data … in parallel" since Howard teaches that the same data is used by each of the processing portions of the ciphering processor. First noted is that Larsen was shown to teach that a packet includes header data and payload data and that authentication operations are performed on the set of header data and payload data of the packets. This point has not been argued. Furthermore, as the claim does not prohibit encryption of both the header data and payload data, both Howard's and Larsen's teachings of encrypting the packet clearly teach "performing encryption operations on a set of data in the payload data”. As to the parallel processing aspect, Howard clearly and explicitly teaches "implementation of ciphering and data integrity operations in parallel" (column 6, lines 16-17).

Applicant goes on to argue that “Howard does not disclose or suggest this communication of data generated by the data integrity function to the ciphering function” with respect to the 3 limitations starting with the combining limitation. However, Fumy was shown to teach these limitations.

Applicant argues that "Fumy, like Howard, fails to disclose "wherein the encryption operations on the set of payload data for the first packet are performed in parallel with the authentication operations for the first packet," and "***combining remaining payload data for the first packet*** with the authentication code for the first packet; adding padding to the combined remaining payload data and authentication code for the first packet to generate a first packet data block …; and performing encryption operations on the first packet data block," As recited in claim 46". As Howard has already been shown to teach the first argued limitation, Fumy need not teach such limitation. Fumy teaches MAC (message authentication code) computations and ciphering. For block ciphering, the message, including the MAC is padded to force the length of the plaintext to be a multiple of the block cipher's block length and the data is encrypted. With respect to the combination, as Howard already teaches performing authentication and encryption operations on the packet in parallel, such parallel processing is within the combination. Even though Fumy does not explicitly refer to parallel processing, in the combination, Fumy's adding of the MAC and padding to the data to be encrypted will be performed after generation of the authentication code and prior to completion of encryption, such that the authentication and encryption operations are still being performed in parallel, but the additional steps of adding the authentication code and padding to the data, then finishing the encryption thereon will be included as well. This is because parallel authentication and encryption are already being performed within the combination, and Fumy's teachings are provided within the combination.

Furthermore, the claim does not state that the remaining payload data cannot be null. Therefore, even if encryption of the entire packet without the authentication code is complete prior to the authentication code being encrypted, this situation still meets the claimed limitation, as the remaining payload could be null if the encrypted payload fits on a block size boundary, for example.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 2, 3, 28-30, 33, 35, 36, and 45-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Howard (U.S. Patent 6,901,516) in view of Larsen (U.S. Patent 7,068,791), Huynh (U.S. Patent 6,983,366), and Fumy (Fumy, Walter, "Internet Security Protocols", 1998, pp. 186-208, obtained from Springerlink).

Regarding Claim 46,

Howard discloses a method for accelerating cryptographic processing of a plurality of data packets according to a network security protocol, comprising:

Receiving, in a chip, data for a first packet from an off-chip processor (Column 5, lines 36-57; off-chip processor sending

packet data to the buffer memory, where it is retrieved by the ciphering processor);

Performing authentication operations on data for the first packet to generate an authentication code (Column 6, lines 16-25; integrity operations);

Performing encryption operations on a set of data in the payload data for the first packet, wherein the encryption operations on the set of payload data for the first packet are performed in parallel with the authentication operations for the first packet (Column 6, lines 16-25; ciphering and integrity operations being performed in parallel);

Receiving, in the chip, data for a second packet (Column 1, lines 6-10; Column 7, lines 33-44; and Column 7, line 66 to Column 8, line 6; processing subsequent packets received serially and interleaved);

Performing authentication operations on a set of data for the second packet (Column 6, lines 16-25);

Performing encryption operations on the authentication code, wherein the authentication code becomes part of the ciphered data stream itself (Column 3, lines 18-20; and Column 4, lines 11-14);

Passing the cryptographically processed first packet from the chip to the off-chip processor (Column 5, lines 46-57; the ciphering

processor sending the data back to the buffer memory, where it is retrieved by the off-chip processor);

Wherein the authentication and encryption operations for the first packet are performed within the chip in a single pass (Column 6, line 58 to Column 7, line 9; parallel processing and explicit recitation of performing encryption and integrity encoding in a single pass); and

Wherein all operations necessary for encrypting and authenticating are performed within the chip (Column 7, line 66 to Column 8, line 6);

But does not appear to explicitly disclose that the packet comprises header data and payload data upon which the authentication operations are performed, combining remaining payload data for the first packet with the authentication code for the first packet, adding padding to the combined remaining payload data and authentication code for the first packet to generate a first packet data block having a predefined length, performing encryption operations on the first packet data block, or that authentication operations on the second packet are performed in parallel with the encryption operations on the first packet data block.

Larsen, however, discloses that packets comprise header data and payload data and that authentication operations are

performed on the set of header data and payload data of the packets (Column 7, lines 6-45). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the secure packet system of Larsen into the ciphering processor of Howard in order to provide multiple authentication codes within each packet, thereby allowing the system to determine whether a message came from a proper sender via the header's authentication code, so as to allow for adaptive retransmission, even when the payload of the packet was received in error (and thus, the packet's authentication code is incorrect).

Huynh, however, discloses that the authentication operations for the second packet are performed in parallel with the encryption operations on the remaining data to be encrypted for the first packet (Column 2, lines 24-35; Column 6, lines 19-38; and Column 8, line 23 to Column 9, line 8). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the packet processing techniques if Huynh into the ciphering processor of Howard as modified by Larsen in order to allow another packet to be processed as soon as a particular resource (encryption or authentication unit) becomes available, so the system need not wait until the first packet is completely processed before beginning processing of another packet, thereby

allowing the system to process network security protocol data faster and more efficiently.

Fumy, however, discloses combining remaining payload data for the first packet with the authentication code for the first packet; adding padding to the combined remaining payload data and authentication code for the first packet to generate a first packet data block having a predefined length; and performing encryption operations on the first packet data block (Pages 198-199; encrypting the entire message, including the MAC, with padding being added to the combination of message and MAC when using a block cipher). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocols of Fumy into the ciphering processor of Howard as modified by Larsen and Huynh in order to provide security using secure, highly-used, and well-known protocols, and/or to gain cryptographic security between two parties and interoperability between differently coded programs.

Regarding Claim 2,

Howard as modified by Larsen, Huynh, and Fumy discloses the method of claim 46, in addition, Fumy discloses that the network security protocol is SSLv3 (Pages 196-197).

Regarding Claim 3,

Howard as modified by Larsen, Huynh, and Fumy discloses the method of claim 46, in addition, Fumy discloses that the network security protocol is TLS (Pages 197-203).

Regarding Claim 28,

Howard as modified by Larsen, Huynh, and Fumy discloses the method of claim 46, in addition, Howard discloses aligning the received set data for the first packet (Column 6, lines 26-47; both MD5 and SHA-1 require padding of the data in order to ensure that the data is a multiple of 512 bits. This can be seen, for example, in the portion of Bruce Schneier's book, Applied Cryptography, as provided by Applicant in the IDS dated 1/21/2003); and Larsen discloses that the set of data comprises header data (Column 7, lines 6-45).

Regarding Claim 29,

Howard as modified by Larsen, Huynh, and Fumy discloses the method of claim 28, in addition, Howard discloses storing the aligned set of data for the first packet to accumulate a predefined amount of data before commencing the authentication operations (Column 6, lines 26-47; as just described, MD5 and SHA-1 require 512 before proceeding); Huynh discloses that the data is stored in a FIFO (Figure 5); and Larsen discloses that the set of data comprises header data (Column 7, lines 6-45).

Regarding Claim 30,

Howard as modified by Larsen, Huynh, and Fumy discloses the method of claim 29, in addition, Howard discloses that the predefined amount of data comprises 512 bits (Column 6, lines 26-47; as just described, MD5 and SHA-1 require 512 before proceeding).

Regarding Claim 33,

Howard as modified by Larsen, Huynh, and Fumy discloses the method of claim 46, in addition, Fumy discloses aligning, for encryption operations, the set of data in the payload data for the first packet to provide the aligned data for the encryption operations (Pages 198-199; padding, for example).

Regarding Claim 35,

Howard as modified by Larsen, Huynh, and Fumy discloses the method of claim 33, in addition, Fumy discloses that aligning, for encryption operations, comprises adding padding (Pages 198-199).

Regarding Claim 36,

Howard as modified by Larsen, Huynh, and Fumy discloses the method of claim 33, in addition, Fumy discloses storing the aligned set of data in the payload data for the first packet for the encryption operations to accumulate a predefined amount of data before commencing the encryption operations (Pages 198-199; when using a block cipher, blocks of the same size are used;

therefore, the encryption operations will proceed once the block size has been filled); and Huynh discloses storing the data in a FIFO (Figure 5).

Regarding Claim 45,

Howard as modified by Larsen, Huynh, and Fumy discloses the method of claim 46, in addition, Huynh discloses receiving, in the chip, encrypted data; performing in an encryption component, decryption on the encrypted data to generate a decrypted data block; and passing the decrypted data block to an authentication component (Column 7, lines 53-63); and Fumy discloses aligning, by the authentication component, the decrypted data block (Pages 198-199).

3. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Howard in view of Larsen, Huynh, and Fumy, further in view of Ganapathy (U.S. Patent 6,557,096).

Howard as modified by Larsen, Huynh, and Fumy discloses the method of claim 1, in addition, Larsen discloses that the header data for the first packet comprises content type and length (Column 7, lines 6-45; and Column 9, lines 1-23); but does not explicitly disclose that the data is aligned into rows of data where each row of data contains a single type of data.

Ganapathy, however, discloses that that the data is aligned into rows of data where each row of data contains a single type of data (Column 17, lines 38-55; and Column 19, line 35 to Column 20, line 25). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data aligner of Ganapathy into the ciphering processor of Howard as modified by Larsen, Huynh, and Fumy in order to properly align and format data before sending it for mathematical (in this case, authentication and encryption/decryption) operations, so that the data has any needed sign and guard bits pre-pended thereto.

4. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Howard in view of Larsen, Huynh, and Fumy, further in view of Gaytan (U.S. Patent 5,638,367).

Howard as modified by Larsen, Huynh, and Fumy does not explicitly disclose that aligning, for encryption operations, comprises removing non-valid data.

Gaytan, however, discloses that aligning, for encryption operations, comprises removing non-valid data (Column 1, line 62 to Column 2, line 29). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data packing system of Gaytan into the ciphering processor of Howard as modified by Larsen,

Huynh, and Fumy in order to gain better throughput and performance by only sending valid data past the buffer.

### *Conclusion*

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ashok Patel can be reached on (571)272-3972. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2491

/Jeffrey D Popham/
Examiner, Art Unit 2491